IN THE UNITED STATES DISTRICT COURT

FOR THE EASTERN DISTRICT OF NORTH CAROLINA

EASTERN DIVISION - Civil Action Number 4:24-CV-00051-M-RN

Cynthia B. Avens (Plaintiff)	)	PLAINTIFF'S MOTION FOR LEAVE TO CONDUCT LIMITED DISCOVERY
Faris C. Dixon, Jr., District Attorney Pitt County Memorial Hospital, Inc. Dr. Karen Kelly, Medical Examiner John/Jane Doe, John/Jane Doe (Defendants)	)	

PLAINTIFF'S MOTION FOR LEAVE TO CONDUCT LIMITED DISCOVERY

INTRODUCTION:

Plaintiff, Cynthia B. Avens ("Avens"), proceeding pro se, respectfully moves this Court for leave to conduct limited discovery pursuant to Rule 26(d) of the Federal Rules of Civil Procedure, and in support thereof states the following:

PURPOSE:

This motion is being submitted to request limited and narrowly tailored discovery in light of recent cyber activity directed at Avens and her digital property. Earlier details based on the information known at the time have been presented to the Court via a court notice, DE 90, and in her response to the defendants' reply to Avens's objection to the Court's Memorandum and Recommendation, DE 89. The cyber breaches and intrusions escalated to outsiders taking full control over Avens's website **and** hosting account, resulting to complete destruction of Aven's website, formerly, Fight Until You Win at fightuntilyouwin.com.

TIMELINE:

March 22, 2024: Avens filed her complaint with the District Court: DE 1.

May 29, 2024: ECU Health filed a motion to dismiss and memorandum in support of; DE 22 & 23. In their memorandum, ECU Health asserted that a 2016 settlement agreement and release ("SAR") barred Avens's current claims.

June 18, 2024: Avens filed her amended complaint: DE 33.

July 16, 2024: ECU Health filed a motion to dismiss and memorandum in support of; DE 49 & 50. In their memorandum, ECU Health again asserted that the SAR barred Avens's current claims.

August 5, 2024: Avens filed her response to ECU Health's motion to dismiss, arguing that they misrepresented the scope of the SAR and provided a copy of a draft SAR as an exhibit to support her argument: DE 57 & 57-1.

August 9, 2024: Counsel for ECU Health attempted to force Avens to strike the draft SAR from the record via a threatening letter sent to her email.

August 22, 2024: Avens filed a motion to determine validity and applicability of the SAR; DE 62.

August 28, 2024: ECU Health filed a motion to seal the SAR and a memorandum in support of; DE 63 & 64.

August 29, 2024: Avens filed her opposition to ECU Health's motion to seal: DE 65.

September 3, 2024: ECU Health filed their response to Avens's motion to determine validity: DE 67. In their response, ECU Health confirmed that while they were not currently using the SAR as a defense, their intent was to use it in the future if prior affirmative defenses failed.

October 8. 2024: A Motions Hearing was held where both parties. Avens and ECU Health expressed their concerns regarding their positions on the SAR; DE 73. ECU Health also agreed to provide a copy of the executed SAR to the Court under seal or for in-camera review.

October 23, 2024: Judge Numbers issued an order for ECU Health to provide a copy of the executed SAR. as well as a memorandum explaining if the public's right to access is based on common law or First Amendment and how ECU Health's interests outweigh that right; DE 74.

November 12, 2024: ECU Health submitted their memorandum explaining that the public does not have a right to access a document not used for adjudication; DE 81.

November 19, 2024: Avens submitted a reply to ECU Health's memorandum explaining that sealing the SAR would violate her First Amendment right to publicly support her argument against ECU Health's statements regarding the scope of the SAR as used in their previous filings; DE 82.

Avens believes it was necessary to include the above timeline as it is relevant to the remaining timeline that follows.

January 3, 2025: Avens filed a Notice Regarding Public Disclosure notifying the Court of her decision to publicly disclose the draft SAR on her former website. Fight Until You Win ("Website"). previously at fightuntilyouwin.com; DE 83. Because the Order issued in October was solely about the public's right to access the SAR. Avens made this decision believing that the Court overlooked her rights to publicly defend against public statements by ECU Health regarding the SAR.

January 15, 2025: Website became inaccessible due to a server issue unrelated to GoDaddy's (Avens's hosting provider) servers.

January 24, 2025: Judge Numbers denied ECU Health's motion to seal the SAR because the document was already made public on Avens's (former) website. He also mentioned that Avens may be sued for publishing the SAR on a public website against the terms of the document's confidentiality clause.

February 3-15, 2025: Eight suspicious subscriber accounts were created on Website's backend. Though Avens retained only 7 of the 8 email notifications sent to her, she believes the 8th account was likely created on February 2, 2025.

February 16, 2025: There was a failed login attempt to the Website's dashboard.

February 18, 2025: Through an unlawful hacking into Avens's website, 18 core files were modified as thousands of lines of code were inserted simultaneously at 12:53pm. To the best of Avens's knowledge, these modifications ensured the perpetrator had a permanent backdoor to the website's administrative dashboard, allowing themselves full control over the website, unlimited access to Avens's hosting account with GoDaddy, how front-facing pages would be viewed, and other illicit activities requiring an IT specialist to decipher. Due to delays in a free version of plugin, Wordfence, this info was not known until April 7, 2025, approximately 30-days after Avens installed it in March 2025.

March 1, 2024: Avens's X account (formerly Twitter) was breached and signed into by someone other than Avens.

March 3, 2025: Avens received an unsolicited email from ECU Health that contained a tracking pixel within its header, sending Avens's IP address and other information to ECU Health. This email was sent directly to Avens despite

- Avens not being a patient of ECU Health;
- Avens not being on any ECU Health mailing list, promotional or otherwise;
- No one outside of ECU Health's risk management and legal teams having access to Avens's email; and
- ECU Health being represented by Counsel, K&L Gates, during the current civil rights case.

March 4, 2025: Avens opened the email, unaware of the tracking pixel it contained.

March 5, 2025: Avens's IP address began showing up in the Website's dashboard metrics as having visited front-facing pages that Avens did not visit herself; nor had anyone in Avens's household accessed the web pages. This IP spoofing continued until at least April 1, 2025, as Avens's online identity was impersonated. During this period, Avens was preparing her DE 95 court submission that had a March 14 deadline. Therefore, she was not tuned in to her website activities until after she mailed her document to the Court.

March 12-13, 2025: Avens began noticing her IP address being used to visit to Website's frontend during occasions when she was:

- on the backend, thus no tracking of her IP address was recorded
- performing other internet activities unrelated to Website
- not actively on the internet at all, including periods of time when she was asleep

The dates of access using Avens's IP address date back to March 5, 2025. Avens confirmed this information by comparing the Website's access using her IP address to her Google history.

March 21, 2025: Avens purchased a 5-year hosting plan to continue her website until March 21, 2030, with GoDaddy.

March 25, 2025: Avens's domain and full domain renewal automatically renewed for another year.

April 1, 2025: The last known IP spoofing occurred.

April 3, 2025: After multiple failed attempts, including attempts that broke her internet, Avens changed her IP Address. This may possibly account for why the IP spoofing ended.

April 6, 2025: Avens continued to take measures to harden her website. One step involved contacting GoDaddy for assistance to remove a "read me" file. During this phone call, Avens's website was deleted. Initially, Avens believed GoDaddy representatives were responsible for the mishap. GoDaddy representatives assumed Avens was responsible for the website removal. Subsequently, GoDaddy restored Avens's website later that day. However, it was not restored to its previous state. Two plugins that Avens previously utilized to monitor site visitations on the front end failed to provide any further metrics. The failures persisted even after Avens re-uploaded clean copies of the plugins. Avens later learned that her hosting account with GoDaddy had been breached. The hacker knew Avens was making changes to harden her website because unbeknownst to Avens, they were already inside her backend. However, they did not know she was on the phone with GoDaddy which is when they apparently removed the website via Avens's GoDaddy dashboard.

April 6, 2025: Avens's GoDaddy account was unlawfully breached by the person with access to the website's dashboard. The following changes were made; however notices were sent to Avens's secondary email account on file with GoDaddy. She did not access these emails until April 9, 2025:

- Wordpress (Avens's website platform build) was removed at 2:17:25pm. In other words, Avens's website was removed.

- Wordpress was removed a second time at 2:48:39pm. Keep in mind that Avens was on the phone with GoDaddy during this time as she waited for answers regarding why GoDaddy needed to restore her site while GoDaddy assumed Avens wanted the site removed.
- The Website's SSL certificate was modified at 6:23:22pm.
- The Website's DNS was modified at 6:23:24pm.
- Website was detected as being down again at 6:26:30pm., likely due to the DNS modification.

April 7, 2025: Avens received notification from a Wordfence security plugin that several of her core files were modified. Upon further research, it confirmed in files retained on GoDaddy's dashboard that the files were actually modified on February 18, 2025, as explained above.

April 7, 2025: Avens began downloading core files as she prepared to move her website from GoDaddy's hosting to another provider. At 11:21pm someone, operating as Avens, using her username and admin privileges in her website's dashboard, downloaded the File Manager plugin & deactivated the same plugin at 11:28pm. Avens went to bed at about 7:00pm as files continued to download on her computer. She was asleep when this occurred. The next morning, April 8, as she attempted to resume downloading files, no files downloaded and all website files disappeared from FileZilla (the app used to download). The File Manager plugin was manipulated to prevent Avens from downloading any further files. Her website had been unlawfully hijacked. Avens went on to transfer her domain to another hosting provider. It was during this time that she realized that a critical file, a wp-content folder had never downloaded prior to the manipulation of the File Manager plugin. Avens lost all the information she had provided to her website. Blog posts, images, documents, etc. were all **GONE.**

April 8, 2025: Someone again accessed Avens's hosting account and made more changes. Email notifications were not checked until April 9.

- Full domain protection that had auto-renewed on March 25, was cancelled at 3:37:37pm.
- The website's SSL certificate was modified at 6:23:13pm.
- Someone accessed the hosting account using a Singapore IP indicating that the perpetrator masked their own IP and location with a VPN at 3:42:59pm.

FEBRUARY 18, 2025, REVISITED

Whoever modified these files wanted total control. This was not a casual breach it was a guaranteed indicator of high-level malicious intent. The simultaneous modifications across 18 core files suggest a pre-planned, pre-scripted attack, likely executed using a multi-file uploader such as FileZilla. Deploying the attack all at once, rather than in phases, minimized the risk of detection and allowed the intruder to seize control before any intervention was possible. This was cyber terrorism, carried out to regain control of the narrative after Avens publicly released the 2016 settlement agreement that ECU Health had misrepresented in court filings. The goal was to silence Avens's constitutionally protected speech and prevent the public from learning the truth about prior misconduct—misconduct that, if fully exposed, could irreparably damage reputations and legal defenses.

Avens does not possess the tools or authority to investigate these cyber-attacks beyond her own digital trail. Without limited, immediate discovery, the evidence necessary to identify the responsible parties and preserve what remains may be permanently lost. Plaintiff seeks only what is necessary to protect the integrity of this case, her digital property, and her personal safety.

THE COURT'S PART IN THIS

- Avens notified the Court that ECU Health misrepresented the scope and legal strength of the SAR. The Court did not address it.
- Avens notified the Court that ECU Health made repeated false statements in DE 60. While unrelated to the SAR, that filing demonstrated the Defendants blatant dishonesty. The Court dismissed her motion to strike and ignored the documented lies.
- Avens asked the Court to determine the validity of the SAR, since ECU Health repeatedly relied on the document when it served their interests. The Court denied the motion, stating it was not properly brought because Avens had not requested leave to amend her complaint—even though Defendants, not Avens, made the SAR central to the dispute.
- Avens asked the Court to address the intimidation tactics used against her after she submitted the SAR as an exhibit to correct the record. The Court justified ECU Health's conduct as a simple effort to protect confidentiality. When Avens raised concerns about being given only three business days to strike the SAR, the Court noted that ECU Health was not required to give any time at all—completely missing the broader issue that, as a pro se litigant, Avens had no knowledge of what a "strike" truly entailed or how to draft a motion to protect her rights. The practical burden of filing by mail or hand delivery was also not considered. Defendants were coddled. Avens was held to standards even K&L Gates has struggled to meet, based on the number of extensions they've requested.
- Avens asked the Court to consider the real-world impact sealing the SAR would have on her ability to defend herself against public falsehoods. The Court instead centered its analysis on whether the public—not the plaintiff—had a Constitutional right to access the document.

- Avens filed a notice after she noticed the first signs of breach to her website, hoping the Court would intervene. The notice was met with silence.

So here we are. Throughout this case, Avens has nearly begged to be heard by this Court. But the Court repeatedly disregarded her position while extending every benefit of the doubt to Defendants. Now, according to the circumstantial evidence, ECU Health—or someone acting on their behalf—felt empowered to retaliate against Avens by shamelessly obliterating her digital property and further violating her constitutional rights.

LEGAL STANDARD AND SCOPE OF REQUESTED DISCOVERY

Under Rule 26(d)(1) of the Federal Rules of Civil Procedure, a party may seek early discovery before the Rule 26(f) conference upon a showing of good cause. Courts have found good cause exists where early discovery is necessary to identify responsible parties, prevent further harm, or preserve evidence at risk of loss or destruction.

Plaintiff meets that standard. She has presented detailed, time-stamped evidence of hacking, digital impersonation, and the complete destruction of her original website, all occurring after the publication of a contested settlement agreement and within the pendency of this lawsuit. The pattern of activity suggests coordinated misconduct, with timing that aligns with procedural events in this case and a clear retaliatory motive.

Plaintiff requests narrowly tailored discovery limited to the following:

- GoDaddy Account Access Records – Subpoena(s) to identify IP addresses used to access Avens's website and GoDaddy hosting dashboard between February 2, 2025 and April 8, 2025; administrative tied to account changes (e.g., SSL, DNS, full domain protection).

- Email Metadata – Subpoena to Constant Contact or related providers for metadata regarding the March 3, 2025, email sent to Plaintiff's address containing a tracking pixel.
- Discovery Directed to ECU Health – Limited written discovery to ECU Health concerning the creation, authorization, and distribution of the March 3, 2025, email, including identification of persons with access to Avens's email and IP data.

This request does not preclude discovery suggestions based on the findings or recommendations of a qualified IT specialist.

CURRENT EVIDENCE

The evidence Avens has on hand at this time will be available upon request if this motion is granted. This includes emails, screenshots, core file downloads, etc.

CONCLUSION

For the reasons stated above, Plaintiff respectfully requests that this Court grant leave to conduct limited discovery. Plaintiff further requests that the Court issue any additional orders it deems necessary to ensure the preservation of evidence and the protection of Plaintiff's constitutional rights.

Respectfully Submitted,

April 14, 2025

/s/ *Cynthia B. Avens*
Cynthia B. Avens
303 Riverside Trail
Roanoke Rapids, NC 27870
Avens1@charter.net
252-203-7107
Pro Se Litigant

CERTIFICATE OF SERVICE

I hereby certify that on April 14, 2025, the Plaintiff's Motion For Leave To Conduct Limited Discovery was shipped by UPS to the U.S. District Court in Greenville, NC. ETA 4/15/2025. Tracking # 1Z9H79KT0300174269. Upon docketing, the CM/ECF system will send electronic notification of filing to the defendants' counsel.

Respectfully submitted 4/14/2025,
/s/ Cynthia B. Avens
Cynthia B. Avens
303 Riverside Trail
Roanoke Rapids, NC 27870
Avens1@charter.net
252-203-7107
Pro Se Litigant

Chris D. Agosto Carreiro
Special Deputy Attorney General
N.C. Department of Justice
P.O. Box 629
Raleigh, NC 27602
ccarreiro@ncdoj.gov
Telephone: (919) 716-6874
Facsimile: (919) 716-6755
State Bar No. 45356
Counsel for DA Dixon

Daniel D. McClurg
K&L Gates LLP
300 South Tryon Street, Suite 1000
Charlotte, North Carolina 28202
daniel.mcclurg@klgates.com
(704) 331-7400
(704) 353-3114
NC Bar #53768
Counsel for Defendant Pitt County Memorial Hospital, Inc.

Jeremy D. Lindsley
Assistant Attorney General
N.C. Department of Justice
P.O. Box 629
Raleigh, NC 27602
jlindsley@ncdoj.gov
Tel: 919-716-6920
Fax: 919-716-6764
NC State Bar No. 26235
Counsel for Dr. Karen Kelly

Terrence M. McKelvey
K&L Gates LLP
501 Commerce Street, Suite 1500
Nashville, Tennessee 37203
terrence.mckelvey@klgates.com
(615) 780-6700
(615) 780-6799
NC Bar #47940
Counsel for Defendant Pitt County Memorial Hospital, Inc.

Elizabeth Curran O'Brien
Special Deputy Attorney General
N.C. Department of Justice
Email: eobrien@ncdoj.gov
Tel: (919) 716-6800
Fax: (919) 716-6755
NC State Bar No. 28885
Counsel for DA Dixon